入侵检测系统分析及其在Linux下的实现（3） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c103_144485.htm 2.4 数据分析模块 数据分析是入侵检测系统的核心。各种分析方法各有利弊，但基于规则的检测方法因为事先将各种入侵方式表示为规则存放于规则库中，因此在规则库比较完备的基础上，可以有很好的检测效率，所以我们在该系统的实现中主要考虑了基于规则的检测方法。 基于规则的检测方法是误用检测的一种。入侵检测系统需要从以往的攻击入侵活动中，归纳识别出对应的入侵模式，并将这些入侵模式存放于规则库中，然后将系统现有的活动与规则库中的规则进行模式匹配，从而决定是否有入侵行为发生。 每一种基于规则的入侵检测方法都需要一个确定的入侵模式库，即规则库，其中存放着描述入侵方法和行为的规则。在我们的系统中，采用了SNORT的入侵行为描述方法。SNORT是一个开放源代码的轻量级的基于网络的入侵检测系统。这种描述方法简单、易于实现，能够描述绝大多数的入侵行为。由于其简单，因此检测速度比较快。 规则库中的每条规则在逻辑上分为两部分：规则头部和规则选项。规则头部包含规则的操作、协议、源IP地址和目标IP地址及其网络掩码和端口。规则选项包括报警信息及需要检测的模式信息。规则的一般格式为： （；；…；；） 在圆括号前的部分是规则头部，在圆括号中的部分是规则选项。规则选项部分中冒号前面的词组称为选项关键字。规则选项不是规则的必需部分，它只是用来定义收集特定数据包的特定特征。一条规则中不同部分必须同时满足才能执行，相

当于“ 与 ”操作。而同一个规则库文件中的所有规则之间相当于一个“ 或 ”操作。 以下是一个例子：alert tcp any any -> 192.168.1.0/24 111 (content:|00 01 86 a5|. msg: mountd access.)。该条规则描述了：任何使用TCP协议连接网络192.168.1.0/24中任何主机的111端口的数据包中，如果出现了二进制数据00 01 86 a5，便发出警告信息mountd access。 规则操作说明当发现适合条件的数据包时应该做些什么。有两种操作：alert和log。如果是 alert，则使用选定的告警方法产生警报，并记录这个数据包；如果是log，则只记录该数据包。 协议指明当前使用的是何种协议。对于IP地址和端口，关键字“ any ”可以用来定义任何IP地址。在IP地址后指定网络掩码，如/24指定一个C类网络，/16指定一个B类网络，/32指定一个特定主机。如192.168.1.0/24指定了从192.168.1.1 到 192.168.1.255的一个范围的IP地址。 IP地址有一个“ 非 ”操作。这个操作符号用来匹配所列IP地址以外的所有IP地址。“ 非 ”操作使用符号“ ！ ”表示。例如任何由外部网络发起的连接可以表示为：alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111。 端口号可以用几种方法指定：用“ any ”、数字、范围以及用“ 非 ”操作符。“ any ”指定任意端口。指定端口范围用“ ： ”它可以指定一个范围内的所有端口。如：log udp any any -> 192.168.1.0/24 1:1024。该条规则记录任何从任意主机发起的到目标网络任何主机上的1～1024端口的UDP协议数据包。 方向操作符“ -> ”规定了规则应用的数据流方向。其左边的IP地址为数据流的起点，右边为终点。双向操作符为“ ”，它告诉系统应该关注任何方向的数据流。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com